*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. I (Jan.- Feb. 2018), PP 35-46*
*www.iosrjournals.org*

# A Survival Study on Energy Efficient And Secured Routing In Mobile Adhoc Network

*C. Daniel Nesa Kumar[1], Dr. V. Saravanan[2]
[1]*Ph.D-Research Scholar, Department Of Computer Science, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India*
[2]*Head and Associate Professor, Department of Information Technology(PG), Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India*
*Corresponding Author: C. Daniel Nesa Kumar*

***Abstract:*** *A mobile ad hoc network (MANET) is an infrastructure-less network where the one mobile device link with other device wirelessly. Each device in MANET changes its movement and links in any direction often. Routing in MANET is the process of sending the information from source to destination node. During routing process, energy consumption and load balancing are the demanding issue to improve the network lifetime. In addition, security plays main part during the data transmission from source node to destination. Secured routing is process of preserving the information from unauthorized users during data transmission in MANET. In existing works, there are many methods for energy efficient and secured routing in MANET. But, the energy consumption and security level was not improved. Our main objective of the paper is to study the existing issues for energy efficient and secured routing in MANET.*

***Keywords:*** *Mobile ad hoc network (MANET), data transmission, secured routing, infrastructure-less network, energy consumption.*

---

Date of Submission: 10-01-2018 Date of acceptance: 16-01-2018

---

## I. Introduction

A MANET is self-organizing network that allows wireless communication between the mobile devices. With the limited resources like power, bandwidth, processing capability, and storage space, it is an essential one to minimize the routing overhead in MANETs and guarantees the high rate of packet delivery. Security in MANET routing protocol is method to transfer the data packet securely. The routing protocols are depending on cryptography scheme, security connection, key distribution, authentication, etc. MANET is the future network as it is versatile, easy to employ, inexpensive and immediately update as well as reconfigure. This paper is ordered as follows: Section II discusses reviews on energy efficient and secured routing in MANET, Section III describes the existing energy efficient load balanced routing with performance analysis comparison, Section IV explains energy efficient multipath and multicast routing and possible comparison, Section V describes the secured routing with result comparison, Section VI explains the limitations as well as future works. Section VII concludes the paper.

## II. Literature Review

Multipath Battery and Mobility-Aware routing scheme (MBMA-OLSR) was designed in [1] depending on MP-OL SRv2. Multi-Criteria Node Rank (MCNR) metric comprised the residual battery energy and node speed. Energy and Mobility Aware Multi-Point Relay (EMA-MPR) selection mechanism was introduced by MBMA-OLSR to contribute MPRs for flooding the information. But, MBMA-OLSR was not appropriate for large-scale network and multi-hop networks. An Intelligent Energy-aware Efficient Routing protocol for MANET (IE2R) was designed in [2] by Multi Criteria Decision Making (MCDM) technique with entropy and Preference Ranking Organization METHod for Enrichment of Evaluations-II (PROMETHEE-II) method to recognize the efficient route. But, the IE2R protocol was not used in heavy traffic conditions. An ant colony-based energy control routing (ACECR) protocol was presented in [3] to find optimal route with encouraging feedback character. Though energy consumption was reduced, load balancing remained unaddressed. But, the energy-efficient secured routing protocol failed to identify the external attacks with lesser energy consumption. Group key distribution was carried out with generated keys through small number of messages and lesser energy consumption. An energy-efficient secured routing protocol was designed in [4] for link and message without depending on third party. A security level was improved through selecting the secure link for routing by Secure Optimized Link State Routing Protocol.

A scheduled-links multicast routing protocol (SLMRP) was introduced in [5] depending on mobility prediction identified multiple scheduled paths between multicast source and destination. Multiple loop-free and node-disjoint paths were recognized for source-receiver pair in route discovery process. However, SLMRP scheduling mechanism failed to balance the load and not appropriate in case of route repair. A game theoretic framework was designed in [7] for stochastic multipath routing. But, the energy consumption was not minimized using game theoretic framework. An efficient and stable multipath routing approach in MANET was introduced in [8] with congestion awareness. The network predicted the residual energy and stability of links in network. The stability of link LET was evaluated through parameters like velocity, direction of nodes, etc. But, the load balancing efficiency was not enhanced by stable multipath routing approach. A QoS-aware metric was calculated in [6] to recognize the stable link depending on link stability factor (LSF). The stability factor was computed by contention count, received signal strength and hop count. The sender node gathered the periodic packets from all adjacent nodes and number of its neighbors. But, the routing overhead was not reduced using LSF. Denial Contradictions with Fictitious Node Mechanism (DCFM) was designed in [9] to prevent from the node isolation attack. The attacker controlled the victim into attacker as multi-point relays (MPR) over communication channel. MPRs were chosen through node as subset of 1-hop neighbors. However, the security level was not improved using DCFM. A secret-common-randomness establishment algorithm was designed in [10] to perform harvesting randomness directly from network routing metadata. The algorithm was based on route discovery phase of an ad-hoc network with Dynamic Source Routing protocol for minimizing the communication overhead. But, the network connectivity was not accepted in secret-common-randomness establishment algorithm. A new method was introduced in [11] for reducing the gray-hole DoS attack. The designed solution failed to assume explicit node collaboration with node internal knowledge gained through routine routing information. However, packet delivery ratio was not enhanced. A new security protocol called Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN) was introduced in [12] to address the node authentication, network access control and secure communication for MANETs. SUPERMAN joined the routing and communication security at network layer to preserve the network. But, the throughput level was not enhanced using the SUPERMAN protocol. Uncertainty Analysis Framework (UAF) computed the network Belief, Disbelief, and Uncertainty (BDU) values in [13]. The UAF framework combined into many trust variants of AODV protocol that employ the direct trust, indirect trust and global trust. But, the trust level was not improved using UAF.

## III. Energy Efficient Routing

MANETs are infrastructure-less networks that are formed by mobile devices with limited battery lifetime. This limited battery capacity in MANETs is essential for consideration of energy-awareness feature. The routing protocols in MANETs include the energy-awareness for increasing the network lifetime by efficiently using available energy.

### 3.1 Energy and mobility conscious multipath routing scheme for route stability and load balancing in MANETs:

Multipath Battery and Mobility Aware-Optimized Link State Routing (MBMA-OLSR) scheme is introduced to identify multiple stable routes that reduce the energy consumption and link failure because of the node mobility in MANETs. The improvements in the proposed scheme reduce energy consumption during data transmission and increase route stability in MANETs. MBMA-OLSR Scheme is a hybrid multipath routing scheme. MBMA-OLSR scheme essentially employs the proactive mechanism to distribute and build topology information with on-demand mechanisms for executing the route computation in conditions when there are data packets to send. MBMA-OLSR scheme used the functionalities of MP-OLSRv2, like topology sensing, route recovery and loop detection. MBMA-OLSR scheme changes two essential functionalities, namely selection of MPRs and identification of multiple paths through incorporating the energy and mobility awareness techniques. The designed scheme minimizes the energy consumption and addressed the challenges incurred by nodes mobility in MANETs. The structure and functionalities with interconnection between many modules of MBMA-OLSR are explained. The node's mobility model is an essential model utilized in MBMA-OLSR to return the speed of nodes that developed in EMA-MPR for selecting the MPRs. The speed of nodes is utilized in evaluation of MCNR metric to rank the stability of nodes depending on residual battery energy, lifetime and mobility. The MBMA-OLSR scheme extract the information on node MCNR metric that included in HELLO and TC messages to formulate nodes susceptible to the medium during topology sensing. MCNR metric is developed to identify the initial costs of links to access their stability by means of link cost function. The cost is enhanced by two incremental cost functions called '$f_p$' and '$f_e$' to identify many disjoint or non-disjoint paths to the destination. The incremental function '$f_p$' increases the costs of arcs that belong to previous path. This will make future paths use different arcs. '$f_e$' is employed to improve the costs of arcs that result in vertices of

previous path 'P'. The route computation is carried out by Multipath Dijkstra Algorithm to choose the multiple best routes between source-destination depending on quality of links in path rather than the shortest paths.

### 3.2 Ant colony-based energy control routing protocol for mobile ad hoc networks under different node mobility models:

An ant colony-based energy control routing protocol (ACECR) discover the optimal route by encouraging feedback character of ACO. Ant Colony optimization (ACO) is computational model of swarm intelligence for attaining efficient solutions to the optimization problems. ACO employs the idea of artificial ants that are analogous to natural ants that are taken as packets in MANETs. In ACO-based routing algorithms, pheromone content select optimal path in the network. ACO is employed to forward the data stochastically. In ACECR protocol, the routing choice is based on number of hops between nodes, node energy and minimum energy of routes. In ACECR, the routing protocol finds the best route with higher energy level than other routes through examination of average energy and minimum energy of paths. ACECR improved the results of AOMDV and EAAR in number of dead nodes and packet loss rate to improve the network lifetime.

### 3.3 Energy Efficient Secured Routing Protocol For Manets

An energy-efficient secured routing protocol is designed to address the energy efficiency and security problems. The main aim of the routing protocol is to present energy efficient secured routing protocol. For improving the security for both link and message without depending on third party, security level was improved through selecting the secure link for routing by means of Secure Optimized Link State Routing Protocol. Every node chooses multipoint relay nodes between one-hop neighbors to reach all two-hop neighbors. The access control entity approves the node identification to the network. The access control entity is signed by public key '$K_i$', private key '$k_i$', and the certificate '$C_i$' needed by an authorized node to attain the group key. Every node preserves a route table with power status as their entry. After choosing the link on need of new route, the nodes power status is checked in its routing table and consequently arise route. The group key distribution is carried out through generated keys with lesser number of messages for minimizing the energy consumption. The group key is changed periodically to avoid unauthorized nodes and similar group key usage more than amount of data. In addition, communication privacy is presented for both message sender and message recipient by means of Secure Source Anonymous Message Authentication Scheme. The message sender or sending node creates a source anonymous message authentication for message to release each message using MES scheme.

### 3.4 Comparison of Energy Efficient Load Balanced Routing Techniques

In order to compare the energy efficient and load balancing routing using different techniques, node speed is taken to perform the experiment. For performing the routing process, parameters such as throughput and packet delivery ratio are used.

#### 3.4.1 Throughput

Throughput is defined as the total number of bits that are successfully received at the server within given period of time. It is measured in terms of Kbits per seconds (Kbits/s). Throughput level is formulated as,

$$Throughput = \frac{Total\ bytes\ received*8}{t-t_f} \qquad (1)$$

From (1), '$t_f$' represents the time of first packet received and '$t$' denotes time of last packet received. When the throughput is higher, the method is said to be more efficient.

**Table 1** Tabulation for Throughput

| Node Speed (m/s) | Throughput (Kbits/s) | | |
|---|---|---|---|
| | MBMA-OLSR Scheme | ACECR Protocol | Energy-Efficient Secured Routing Protocol |
| 5 | 47 | 42 | 35 |
| 10 | 49 | 45 | 33 |
| 15 | 48 | 43 | 31 |
| 20 | 45 | 42 | 29 |
| 25 | 44 | 40 | 28 |
| 30 | 42 | 38 | 26 |
| 35 | 40 | 36 | 24 |
| 40 | 39 | 35 | 23 |
| 45 | 38 | 33 | 21 |
| 50 | 36 | 31 | 19 |

Table 1 describes the throughput comparison for three different techniques namely Multipath Battery and Mobility Aware-Optimized Link State Routing (MBMA-OLSR) scheme, Ant Colony-based Energy Control Routing Protocol (ACECR) and Energy-Efficient Secured Routing Protocol. In the table 1, throughput of these techniques is compared for different node speed. When the node speed gets increased, the throughput level gets decreased correspondingly. The graphical representation of throughput for different techniques is explained in figure 1.

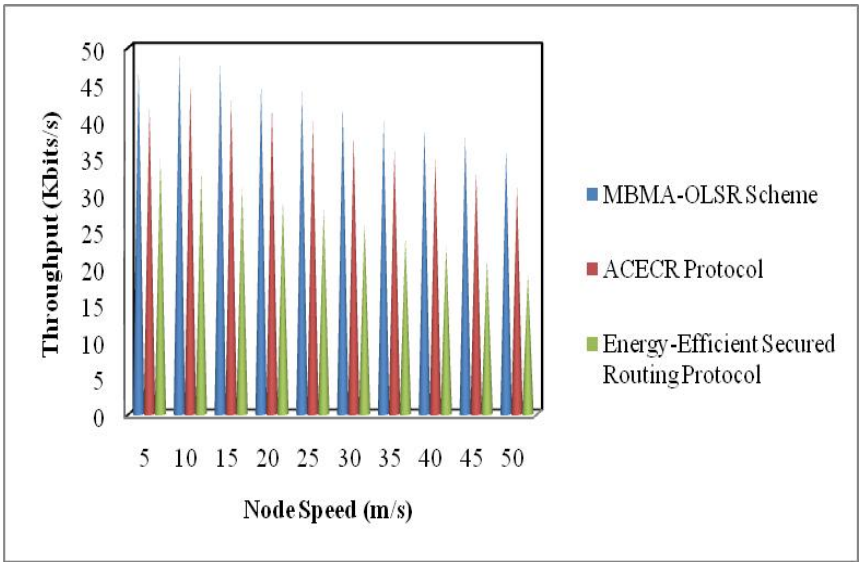


**Fig. 1** Measure of Throughput

Figure 1 describes the throughput comparison for three different techniques, namely MBMA-OLSR scheme, ACECR and Energy-Efficient Secured Routing Protocol. From the figure, it is clear that throughput level of MBMA-OLSR scheme is higher than ACECR and Energy-Efficient Secured Routing Protocol. In MBMA-OLSR scheme, Multipath Dijkstra Algorithm is used to choose the multiple best routes between source-destination. This in turn helps to increase the throughput level. The throughput level of MBMA-OLSR scheme is 11 % higher than ACECR and 65 % higher than Energy-Efficient Secured Routing Protocol.

3.4.2 **Packet Delivery Ratio (PDR**)

Packet Delivery Ratio is defined as rate at which number of data packets that are correctly delivered to the number of data packets sent by source nodes. PDR is measured in terms of percentage (%). The mathematical formula of packet deliver ratio is formulated as,

$$Packet\ Delivery\ Ratio = \frac{Number\ of\ packets\ correctly\ delivered}{Number\ of\ packets\ sent} * 100 \qquad (2)$$

From (2), the packet delivery ratio is measured. When the packet delivery ratio is higher the method is said to be more efficient.

**Table 2** Tabulation for Packet delivery Ratio

| Node Speed (m/s) | Packet delivery Ratio (%) | | |
|---|---|---|---|
| | MBMA-OLSR Scheme | ACECR Protocol | Energy-Efficient Secured Routing Protocol |
| 5 | 85 | 93 | 81 |
| 10 | 80 | 87 | 78 |
| 15 | 74 | 83 | 71 |
| 20 | 72 | 75 | 65 |
| 25 | 67 | 71 | 60 |
| 30 | 62 | 68 | 57 |
| 35 | 58 | 65 | 54 |
| 40 | 55 | 63 | 49 |
| 45 | 52 | 60 | 47 |
| 50 | 50 | 58 | 43 |

Table 2 describes the comparison of packet delivery ratio for different node speed using three different techniques namely Multipath Battery and Mobility Aware-Optimized Link State Routing (MBMA-OLSR)

scheme, Ant Colony-based Energy Control Routing Protocol (ACECR) and Energy-Efficient Secured Routing Protocol. When the node speed gets increased, the packet delivery ratio gets decreased correspondingly. The performance results of packet delivery ratio for different techniques are explained in figure 2.

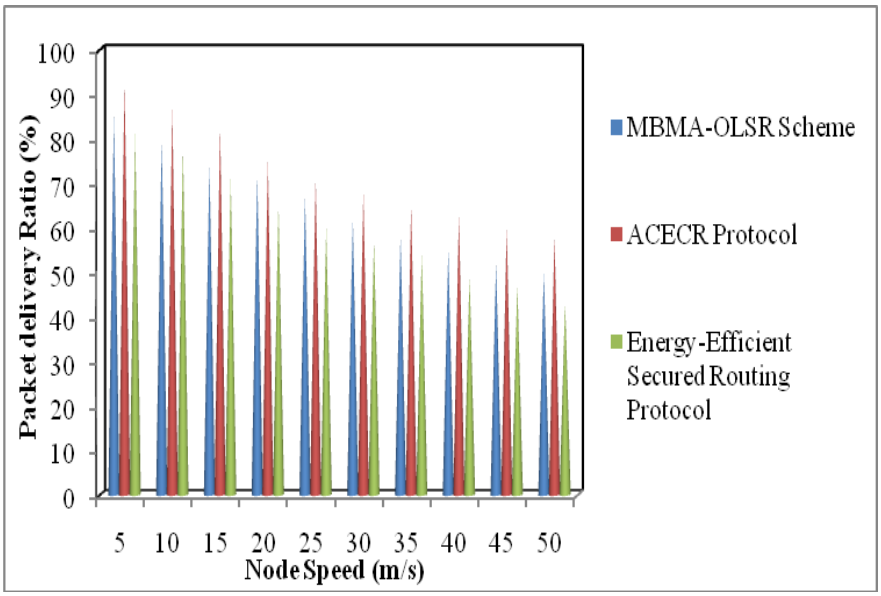


**Fig. 2** Measure of Packet Delivery Ratio

Figure 2 portrays the packet delivery ratio comparison for three different techniques, namely MBMA-OLSR scheme, ACECR and Energy-Efficient Secured Routing Protocol. From above mentioned graph, it is observed that packet delivery ratio of ACECR is higher than MBMA-OLSR scheme and Energy-Efficient Secured Routing Protocol. In ACECR, pheromone content selects the best paths in given network. In addition, ACO forwards the data stochastically. This in turn helps to increase the packet delivery ratio. The packet delivery ratio of ACECR is 11 % higher than MBMA-OLSR scheme and 21 % higher than Energy-Efficient Secured Routing Protocol.

## IV. Energy Efficient Multipath And Multicast Routing

Energy efficient routing is an essential one for MANETs as the mobile nodes are powered by batteries with lesser capacity. Energy-efficient routing protocols diminish the communication energy to transmit and receive data packets. Multipath routing is routing technique with multiple paths through network to avoid fault tolerance, higher bandwidth and security. Multicast is a collection communication where the data transmission is addressed to the group of destination at the same time. Multicast are one-to-many or many-to-many distribution.

### 4.1 Scheduled-Links Multicast Routing Protocol in MANETs

A new multicast routing protocol depending on mobility prediction called scheduled-links multicast routing protocol (SLMRP) is introduced in MANETs. SLMRP finds many scheduled paths among sources and receivers. SLMRP scheduled paths are depending on reliability and quality of service needs in load-balance strategy. Multiple loop-free and node-disjoint paths are identified for every source-receiver pair during route discovery process. One control signaling is employed to construct and schedule multiple paths to receiver. The routes to serve data packet forwarding are scheduled depending on cooperation process between sources and receivers. The set of discovering paths are scheduled to load balance and traffic distribution between paths. Load balance and traffic distribution is attained in SLMRP through controlling path utilization time for every source-receiver pair. Path utilization time is managed through computing the multicast routing activation timers (MRATs) and path timeout timers (PTTs) consistent with route expiration time for the paths. SLMRP route discovery mechanism guarantees loop-free and node-disjoint paths to increase reliability and robustness.

### 4.2 A game theoretic framework for stochastic multipath routing in self-organized MANETs

A game theoretic framework is designed for finding multiple paths between source–destination pair in MANET by considering different routing metrics. In every slot of routing game, a path is selected from constructed multiple paths. The overall performance of routing protocol increases in terms of bandwidth utilization, end-to-end delay, routing overhead and packet delivery ratio. The designed scheme guarantees the

data routing security while data packets are routed through selected paths stochastically in various time slots of routing game. The data routing problem is considered as non-cooperative zero-sum stochastic multipath discrete time routing game for dynamic interactions in MANET. The path variation and time variation at various stages of routing game is employed to counter the attacks for guaranteeing the reliable data flow in MANETs. Residual bandwidth of links between two nodes and surveillance of attackers actions are used as states of routing game. The payoff of game is bandwidth utilization of path from the source to destination in every time slot. An optimal stochastic approximation is employed to find out the value function for optimal routing strategy. Minimax-Q learning is employed to choose an optimal routing plan for increasing the expected sum of discounted payoff.

### 4.3 Energy-efficient stable multipath routing in MANET

An Energy-Efficient and Stable Multipath Routing (EESMR) approach is introduced in MANET with congestion awareness. In the designed approach, network computes the residual energy and stability of links. While calculating the residual energy, it compares with the receiving energy and transmitting energy of node. The stability of link LET is calculated. LET is attained with help of motion parameters (i.e. velocity, node direction). Depending on parameters, the network chooses the path to transmit the data packets between the nodes. The designed approach chooses the best path depending on the factors. The battery level of nodes is considered in the network for improving the performance of throughput and efficiency.

### 4.4 Comparison of Energy Efficient Load Balanced Multipath and Multicast Routing Techniques

In order to compare the energy efficient load balanced multipath routing using different techniques, node speed and routing stage is taken to perform the experiment. For performing the routing process, parameters such as average residual energy and routing overhead are taken.

#### 4.4.1 Average Residual Energy ( $E_{res}$)

The average residual energy is defined as amount of remaining energy left after routing the packets to the neighboring node. It is measured in terms of Joules (J). The average residual energy is mathematically formulated as,

$$E_{res} = \frac{E_{old} * n * E_r}{n+1} \qquad (3)$$

From (3), '$E_{old}$' denotes average energy field of RREQ received by the intermediate node. '$E_r$' represent the remaining energy after sending the route request. '$N$' symbolizes number of hops.

**Table 3** Tabulation for Average Residual Energy

| Node Speed (m/s) | Average Residual Energy (J) | | |
|---|---|---|---|
| | SLMRP | SMR Protocol | EESMR Approach |
| 2 | 4.6 | 3.2 | 5.8 |
| 4 | 4.2 | 2.8 | 5.1 |
| 6 | 4.3 | 2.6 | 5.2 |
| 8 | 4.6 | 2.7 | 5.5 |
| 10 | 4.1 | 2.5 | 5.3 |
| 12 | 3.9 | 2.4 | 5.2 |
| 14 | 4.2 | 2.6 | 5.4 |
| 16 | 4.0 | 2.5 | 5.3 |
| 18 | 4.3 | 2.9 | 5.6 |
| 20 | 4.1 | 2.4 | 5.4 |

Table 3 explains the comparison of average residual energy for different node speed. The table describes the average residual energy comparison for three techniques, namely scheduled-links multicast routing protocol (SLMRP), Stochastic Multipath Routing (SMR) and Energy Energy-Efficient and Stable Multipath Routing (EESMR) approach. When the node speed gets increased, the average residual energy gets decreased correspondingly. The graphical representation of average residual energy for different techniques is explained in figure 3.

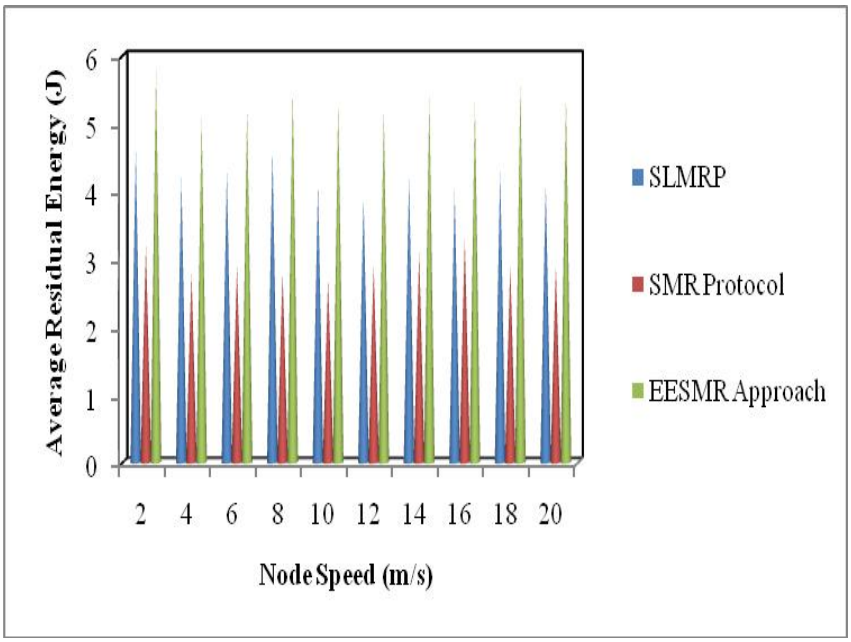


**Fig. 3** Measure of Average Residual Energy

Figure 3 explains the average residual energy comparison for three different techniques, namely SLMRP, SMR Protocol and EESMR Approach. From figure, it is clear that average residual energy of EESMR Approach is higher than SLMRP and SMR Protocol. In EESMR, it compares with the receiving energy and transmitting energy of node for calculating the residual energy. This in turn helps to improve the performance of average residual energy. The average residual energy of EESMR approach is 27 % higher than SLMRP and 83 % higher than SMR Protocol.

4.4.2 **Routing Overhead (RO)**

Routing overhead is defined as the number of error control packets found during the data transmission in MANET. It is measured in terms of second (s). The routing overhead is mathematically formulated as,

$$RO = \sum_{i=1}^{n} NN_i * Time \quad (4)$$

From (4), '$NN_i$' denotes the neighboring mobile node. When the routing overhead is lesser, the method is said to be more efficient.

**Table 4** Tabulation for Routing Overhead

| Routing Stage (Number) | Routing Overhead (second) | | |
|---|---|---|---|
| | SLMRP | SMR Protocol | EESMR Approach |
| 1 | 4.3 | 2.0 | 3.6 |
| 2 | 4.5 | 2.5 | 3.9 |
| 3 | 4.6 | 2.4 | 4.1 |
| 4 | 4.4 | 2.6 | 4.2 |
| 5 | 4.6 | 2.5 | 4.4 |
| 6 | 4.7 | 2.6 | 4.6 |
| 7 | 4.5 | 2.7 | 4.5 |
| 8 | 4.4 | 2.5 | 4.3 |
| 9 | 4.6 | 2.8 | 4.4 |
| 10 | 4.5 | 2.7 | 4.2 |

Table 4 explains the comparison of routing overhead for every routing stage using three techniques, namely scheduled-links multicast routing protocol (SLMRP), Stochastic Multipath Routing and Energy Energy-Efficient and Stable Multipath Routing (EESMR) approach. The graphical representation of routing overhead for different techniques is explained in figure 4.

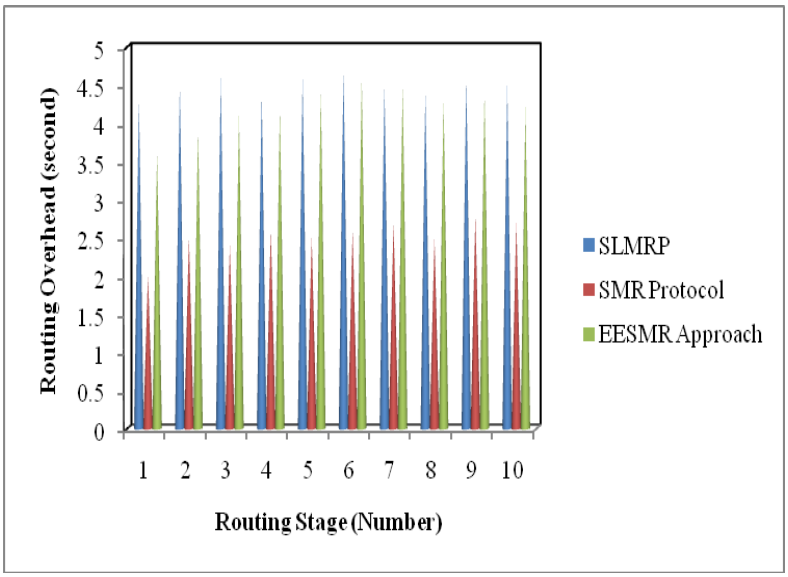


**Fig.** 4 Measure of Routing Overhead

Figure 4 describes the routing overhead comparison for three different techniques, namely SLMRP, SMR Protocol and EESMR Approach. The routing overhead of SMR Protocol is lesser than SLMRP and EESMR Approach. SMR Protocol guarantees the data routing security while data packets are routed through selected paths stochastically in various time slots of routing game. This process results in minimization of routing overhead. The routing overhead of SMR Protocol is 44 % lesser than SLMRP and 40 % lesser than EESMR Approach.

## V. Routing Security

The secured ad hoc routing protocols is used to preserve the routing messages, to avoid attackers from changing the messages or injecting the harmful routing messages into network. Confidentiality is assured but overhead is not reduced. Route establishment are their fast process. When security mechanisms are constructed, the efficiency of routing protocol is sacrificed.

### 5.1 Secret Common Randomness from Routing Metadata in Ad-Hoc Networks

A secret-common-randomness establishment algorithm is introduced for ad-hoc networks. The designed algorithm functions by harvesting randomness directly from network routing metadata through attaining the pure randomness generation and secret-key agreement. The randomness intrinsic in ad-hoc network is collected for creating the secret keys between pairs of nodes that participate in routing process. The designed algorithm depends on route discovery phase of ad-hoc network developing Dynamic Source Routing protocol. In addition, lower bound and an upper bound on attainable number of shared secret bits are computed by adversary's beliefs. It is lightweight and needs relatively lesser communication overhead. The algorithm is estimated for many network parameters in OPNET ad-hoc network simulator.

### 5.2SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks

A new secure framework (SUPERMAN) is introduced to allow network and routing protocols to execute their functions for node authentication, access control, and communication security mechanisms. SUPERMAN joins the routing and communication security at network layer. SUPERMAN protocol is exploited for routing or for providing the communication security to protect the network. SUPERMAN functions at network layer of OSI model. SUPERMAN is introduced to present secured communication framework for MANETs without modification of routing protocol. The data flow from transport layer through network layer to the data link layer. The dashed boxes represent the elements of SUPERMAN for improving confidentiality and integrity. SUPERMAN is used for the node authentication.The key aim of SUPERMAN is to secure the access of virtually closed network (VCN) for expedient, reliable communication with confidentiality, integrity and authenticity services. SUPERMAN identifies eight security dimensions in X.805. SUPERMAN employs collection of security services for MANETs. It fulfils more core services in X.805 than IPsec because of network focused than end to-end oriented. IPsec presented secure environment between two end-points irrespective of route for MANET security. SUPERMAN increases the security of data communicated over MANET. It aims attributes of MANETs and not suitable for other types of network.

**5.3 Uncertainty analysis framework for trust based routing in MANET**

An Uncertainty Analysis Framework (UAF) is designed for MANET for modeling the uncertainty in network. UAF computes the network Belief, Disbelief and Uncertainty (BDU) through contributing the nodes activities. UAF with trust based variants of AODV employed the direct trust, indirect trust and global trust for evaluating the result of different trust models on network Belief, Disbelief and Uncertainty. Many trust based routing plan on BDU revealed by network is examined by test conditions. A trust based routing strategies are employed to increase the network belief in existence of selfish nodes.Central Node receives evidences from participating nodes based on the packet forwarding behavior. CN determines the participating node belief, disbelief and uncertainty values. AODVCN utilizes the CN recommendations for taking the routing decisions. AODVCN is efficient for network where the nodes move slowly, density is minimal and simulation duration is better. AODVIT is efficient in network where the node movements are faster, network is dense and network lifetime is lesser.

**5.4 Comparison of Secured Routing Techniques**

In order to compare the secured routing using different techniques, number of selfish nodes and tasks is taken to perform the experiment. For performing the routing process, parameters such as end-to-end delay and number of kilo bytes for security overhead are taken.

**5.4.1 End-to-End Delay**

End-to-end delay is described as time difference of initial bit of packet sent from source node and last bit of the similar packet is received by sink node. The end to end delay is measured in terms of milliseconds (ms).

$$End\ to\ End\ delay\ (ms) = Starting\ time\ of\ first\ bit\ of\ the\ \ packet - recieving\ time\ of\ \ last\ bit\ of\ \ same\ packet \quad (5)$$

When the end-to-end delay is lesser, the method is said to be more efficient.

**Table 5** Tabulation for End-to-End Delay

| Number of Selfish Nodes (Number) | End-to-End Delay (ms) | | |
|---|---|---|---|
| | Secret-Common-Randomness Establishment Algorithm | SUPERMAN Framework | UAF |
| 10 | 1750 | 1880 | 1910 |
| 20 | 1400 | 1540 | 1610 |
| 30 | 1350 | 1480 | 1520 |
| 40 | 1490 | 1600 | 1720 |
| 50 | 1560 | 1750 | 1800 |
| 60 | 1780 | 1860 | 1990 |
| 70 | 1600 | 1690 | 1780 |
| 80 | 1800 | 1910 | 2090 |
| 90 | 1980 | 2140 | 2220 |
| 100 | 2050 | 2280 | 2350 |

Table 5 describes the comparison of end-to end delay for number of selfish nodes using three techniques, namely Secret-Common-Randomness Establishment Algorithm, Secure framework (SUPERMAN) and Uncertainty Analysis Framework (UAF). When number of selfish nodes gets increased, the routing overhead gets increased correspondingly. The graphical representation of end-to-end delay for different techniques is explained in figure 5.

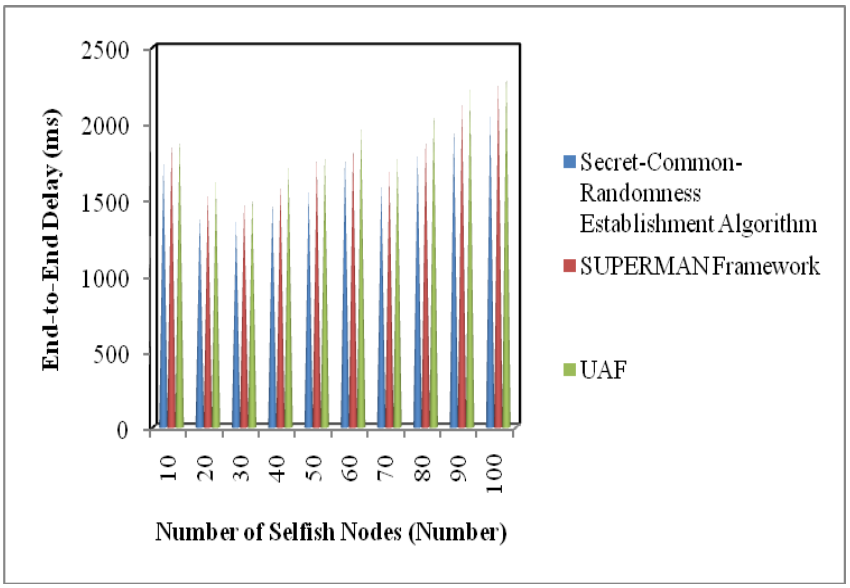


**Fig. 5** Measure of End-to-End Delay

Figure 5 describes the end-to-end delay comparison for three different techniques, namely Secret-Common-Randomness Establishment Algorithm, SUPERMAN and UAF. The end-to-end delay of Secret-Common-Randomness Establishment Algorithm is lesser than SUPERMAN and UAF. Secret-Common-Randomness Establishment Algorithm functions by harvesting randomness directly from network routing metadata through attaining randomness generation and secret-key agreement. This in turn helps to reduce the end-to-end delay. The end-to-end delay of Secret-Common-Randomness Establishment Algorithm is 8 % lesser than SUPERMAN and 12 % lesser than UAF.

5.4.2 **Number of Kilo Bytes for Security Overhead (SO)**

Number of Kilo Bytes for Security Overhead is defined as number of kilobytes required for routing with minimal security overhead. It is measured in terms of numbers.

$$SO = \frac{\left(f(c)*\left(n(n-1)\right)\right)*(h+t)}{p} \qquad (6)$$

From (6), '$f(c)$' denotes the number of rounds needed by given consensus based distributed task allocation algorithm. The number of nodes is denoted by n. The header and tag size are denoted as 'h' and't' respectively. When the number of kilo bytes for security overhead is lesser, the method is to be more efficient.

**Table 6** Tabulation for Number of Kilo Bytes for Security Overhead

| Number of Tasks (Number) | Number of Kilo Bytes for Security Overhead (Number) | | |
|---|---|---|---|
| | Secret-Common-Randomness Establishment Algorithm | SUPERMAN Framework | UAF |
| 10 | 3.2 | 3 | 3.9 |
| 20 | 4.5 | 4 | 4.8 |
| 30 | 5.1 | 4.5 | 5.1 |
| 40 | 5.8 | 5 | 6.3 |
| 50 | 6.1 | 5.5 | 6.5 |
| 60 | 6.5 | 5.9 | 6.9 |
| 70 | 6.6 | 6.2 | 7.5 |
| 80 | 7.2 | 6.5 | 8.1 |
| 90 | 7.4 | 6.9 | 8.8 |
| 100 | 7.8 | 7.3 | 9.1 |

Table 6describes the comparison of number of kilo bytes for security overhead for number of tasks using three techniques, namely Secret-Common-Randomness Establishment Algorithm, Secure framework (SUPERMAN) and Uncertainty Analysis Framework (UAF). When number of tasks gets increased, the number of kilo bytes for security overhead gets increased correspondingly. The graphical representation of number of kilo bytes for security overhead for different techniques is explained in figure 6.

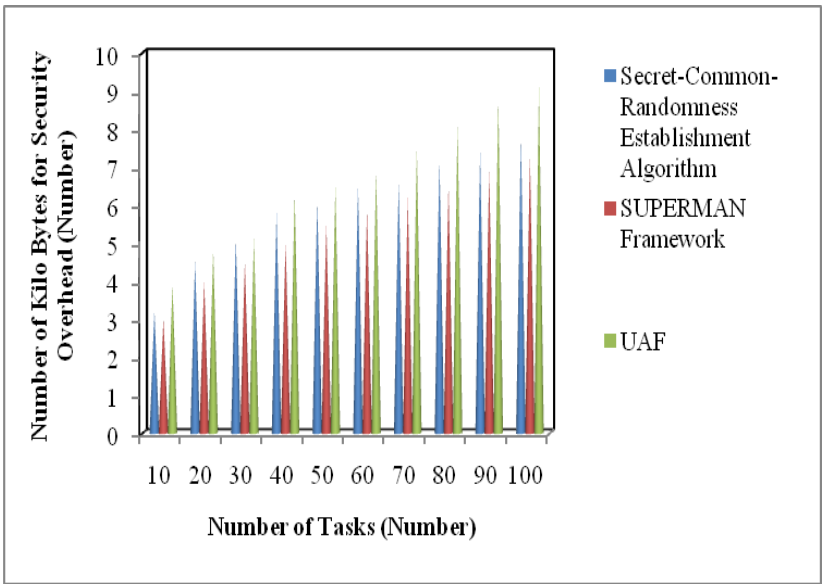


**Fig. 6** Measure of Number of Kilo bytes for Security Overhead

Figure 6 explains the number of kilo bytes for security overhead comparison for three different techniques, namely Secret-Common-Randomness Establishment Algorithm, SUPERMAN and UAF. The number of kilo bytes for security overhead of SUPERMAN is lesser than Secret-Common-Randomness Establishment Algorithm and UAF. SUPERMAN allows network and routing protocols to present their functions for node authentication, access control, and communication security mechanisms. SUPERMAN joins routing and communication security at network layer. This in turn helps to reduce the number of kilo bytes for security overhead. The number of kilo bytes for security overhead of SUPERMAN is 9 % lesser than Secret-Common-Randomness Establishment Algorithm and 18 % lesser than UAF.

## VI. Limitations

MBMA-OLSR routing scheme recognizes the multiple stable routes with minimal energy consumption and link failure due to the node mobility in MANETs. MBMA-OLSR was not appropriate for large-scale network and multi-hop networks. ACECR minimized the balanced energy consumption and increased the network lifetime. Though the energy consumption was minimized, load balancing remained unaddressed. Energy-efficient secured routing protocol selects a secured link for routing without considering third party. The energy-efficient secured routing protocol failed to identify the external attacks with lesser energy consumption.SLMRP scheduled paths improves the reliability and quality of service needs in load-balance strategy. SLMRP scheduling mechanism failed to balance the load and not suitable incase of route repair. In game theoretic framework, the data flow takes place stochastically through many paths between source–destination pair to avoid the attackers. Energy consumption was not reduced using game theoretic framework. An efficient and stable multipath routing approach avoids the data packets losses and occurrence of congestion issue in MANETs. The load balancing efficiency was not improved using efficient and stable multipath routing approach.Secret-common-randomness establishment algorithm depends on route discovery phase of ad-hoc network with Dynamic Source Routing protocol. The network connectivity or traffic load balancing settings were not accepted in secret-common-randomness establishment algorithm. SUPERMAN allows secure access and reliable communication. SUPERMAN targets attributes of MANETs and it is not suitable for additional types of network. Throughput level was not improved using the SUPERMAN protocol.

## VII. Conclusion

A comparison of different techniques for energy efficient and secured routing is carried out. From the survival study, it is clear that MBMA-OLSR routing scheme was not appropriate for large-scale network and multi-hop networks. Energy-efficient secured routing protocol failed to recognize the external attacks with lesser energy consumption. The traffic load balancing settings were not accepted in secret-common-randomness establishment algorithm. SUPERMAN targets MANET attributes and it is not suitable for additional types of network. Throughput level was not improved using the SUPERMAN protocol. The wide range of experiments on existing techniques analyzes the comparative performance of various energy efficient and secured routing techniques and its drawbacks. Finally, from the result, the research work can be carried out to minimize the energy consumption and improve the security level in future.

## References


[1]. Waheb A. Jabbar, Mahamod Ismail and Rosdiadee Nordin, "Energy and mobility conscious multipath routing scheme for route stability and load balancing in MANETs", Simulation Modelling Practice and Theory, Elsevier, Volume 77, 2017, Pages 245–271

[2]. Santosh Kumar Das and Sachin Tripathi, "Intelligent energy-aware efficient routing for MANET", Wireless Networks, Springer, 2017, Pages 1-21

[3]. Jipeng Zhou, Haisheng Tan, Yuhui Deng, Lin Cui and Deng Deng Liu, "Ant colony-based energy control routing protocol for mobile ad hoc networks under different node mobility models", EURASIP Journal on Wireless Communications and Networking, Springer, Volume 2016, Issue 105, 2016, Pages 1-8

[4]. Santosh Kumar Das and Sachin Tripathi, "Energy efficient secured routing protocol for MANETs", Wireless Networks, Springer, Volume 23, Issue 4, May 2017, Pages 1001–1009

[5]. Hasan Abdulwahid, Bin Dai, Benxiong Huang, and Zijing Chen, "Scheduled-Links Multicast Routing Protocol in MANETs", Journal of Network and Computer Applications, Elsevier, Volume 63, March 2016, Pages 56–67

[6]. Gaurav Singal, Vijay Laxmi, M.S. Gaur, Swati Todi, Vijay Rao, Meenakshi Tripathi, Riti Kushwaha, "Multi-constraints Link Stable Multicast Routing Protocol in MANETs", Ad Hoc Networks, Elsevier, Volume 63, August 2017, Pages 115-128

[7]. Sajal Sarkar and Raja Datta, "A game theoretic framework for stochastic multipath routing in self-organized MANETs", Pervasive and Mobile Computing, Elsevier, Volume 39, August 2017, Pages 117-134

[8]. A. Pratapa Reddy and N. Satyanarayana, "Energy-efficient stable multipath routing in MANET", Wireless Networks, Springer, Volume 23, Issue 7, October 2017, Pages 2083–2091

[9]. Nadav Schweitzer, Ariel Stulman, Asaf Shabtai and Roy David Margalit, "Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes", IEEE Transactions on Mobile Computing, Volume 15, Issue 1, January 2016, Pages 163-172

[10]. Mohammad Reza Khalili Shoja, George Traian Amariucai, Shuangqing Wei and Jing Deng, "Secret Common Randomness from Routing Metadata in Ad-Hoc Networks", IEEE Transactions on Information Forensics and Security, Volume 11, Issue 8, 2016, Pages 1674 – 1684

[11]. Nadav Schweitzer, Ariel Stulman, Asaf Shabtai and Roy David Margalit, "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks", IEEE Transactions on Mobile Computing, Volume 16, Issue 8, August 2017, Pages 2174 – 2183

[12]. Darren Hurley-Smith, Jodie Wetherall and Andrew Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks", IEEE Transactions on Mobile Computing, Volume 16, Issue 10, October 2017, Pages 2927-2940

[13]. Sandeep A. Thorat and Prakash J. Kulkarni, "Uncertainty analysis framework for trust based routing in MANET", Peer-to-Peer Networking and Applications, Springer, Volume 10, Issue 4, July 2017, Pages 1101–1111


C. Daniel Nesa Kumar."A Survival Study on Energy Efficient And Secured Routing In Mobile Adhoc Network." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 35-46.